Domain Name Hijacking, Reverse Hijacking, And What To Do If Your Domain Name Is Stolen



Michael Gargiulo, CEO at VPN.com
Published: December 15, 2022 2:08PM EST
Last Updated: July 15, 2023 12:00PM EST

Premium Domain Broker Service

Acquire your perfect domain – even if it's taken.

We paid $1m for VPN.com and now we want to help you. From startups to fortune 100 companies, VPN.com is a leading global domain broker.

What can we help you with today?

Buy Sell

Enter a domain name to search Search

No credit card required. No cost to start. Only pay when we deliver.

In this article

1. Sign up with our #1 choice
2. What Is Domain Name Hijacking?
3. The Risks Of Domain Name Hijacking
4. Reverse Domain Name Hijacking
5. Protect Your Domain Names
6. My Domain Name Was Stolen. What Next?
7. Get Help Recovering Your Stolen Domain Name

RELATED ARTICLES

Hit.com Just Listed For Sale
Marine.com Just Listed For Sale
445.com Just Listed For Sale
The World's Top 30 Domain Brokers
Bahrain Domain Names
Confidential Domain Broker – Private Domain Name Services
Executive & Corporate Acquisition Services

FEATURED

VPN.COM

Acquire Your Premium Domain

today at VPN.com

- Experts in Premium Domains
- Ultra-Secure Transactions
- Commissions Starting at 15%
- Paid $1m for VPN.com
- Only Pay When We Succeed for You
- Completely Confidential

Good domain names are always valuable assets with many selling for thousands or even millions of dollars. This alone is a sufficient reason for malicious actors to target domain names for attack and often motivates domain name hijacking.

However domain name hijacking is especially appealing to hackers when the website is highly valuable to the owner. **In this case they may exploit the importance of the domain name to blackmail the legitimate owner.**

As a webmaster it is essential that you understand the threats that target your domain names and understand how to protect yourself from them. Most attacks fall under one of two umbrellas, domain name hijacking and reverse domain name hijacking.

VPN.COM

Sign up with our #1 choice

- Experts in Premium Domains
- Ultra-Secure Transactions
- Commissions Starting at 15%
- Paid $1m for VPN.com
- Only Pay When We Succeed for You
- Completely Confidential Transactions

Acquire Your Premium Domain

What Is Domain Name Hijacking?



Domain name hijacking is any case of someone stealing a domain name that someone else is the rightful owner of. In general, domain name hijacking occurs as a result of a malicious actor exploiting a vulnerability such as weak passwords and email leaks. However, targeted attacks are also on the rise, as the domain names of eCommerce operations, financial institutions, and other businesses are particularly fruitful targets. The first step in protecting yourself from domain name hijacking is understanding how you can come to be a victim of it, and taking preventative steps.

How Domain Hijacking Occurs

The how of domain name hijacking is fairly complex, as both domain name owners and registrars can make mistakes that enable attacks. Some methods of theft explicitly target the registrar, while others aim at gaining access to your network.

Identity Fraud

Data protection systems at smaller or third-party registrars may be more prone to flaws. An adversary could take advantage of this by pretending to the registrar that they are the legitimate owner but have forgotten their credentials.

> The name of your first pet or your mother's maiden name can be among the security questions asked by some websites.

The answers to this kind of question are particularly simple to learn, so would-be hackers can use them to get access to your account with minimal effort. Choose a registrant that has strong security features and don't take your online safety for granted.

Social Engineering Attacks

If you own one or more valuable domain names, then you're a potential target for social engineering attacks. Today, encryption and website security are usually quite formidable, so malicious actors typically target the weak link; people. Everyone can make a mistake or be tricked from time to time, and this is what a domain hijacker will have in mind when applying techniques like phishing. Be wary of the domain name hijacking most common or dangerous social engineering techniques to avoid having your login data stolen.

Email Hacking

If someone can access part of your login data it is likely that they will be able to access your registrant account and steal your domain names. A person might steal your email with social engineering techniques and use this to access the account or they could steal your email in other ways. This is one of the biggest reasons why Domain Name Hijacking is taking place and becoming usual for businesses.

In particular it is important to be aware of major email leaks and other risk factors that might compromise your information. Remain aware of major leaks among websites you use such as the infamous Yahoo! data leaks. If you have any reason to believe that your passwords are insecure immediately change the login information on all of your important accounts.

Illegitimate Domain Name Transfers

Once someone steals your domain name, they have many options at hand to complicate matters. It's possible for them to cancel your account through the registrar you've used and take the domain name to a different company. **In the worst cases, domain name hijacking cases might involve the thief transferring your domain name to a domain name registrar overseas, outside the jurisdiction of your country.**

Since IP and domain name law can vary from one nation to the other, this can rule out many methods of recourse. While ICANN, the international body that governs domain names may still be able to help, your situation is much more difficult once someone has successfully stolen your IP.

The Risks Of Domain Name Hijacking



Like any valuable good, a hijacker might attempt to resell your domain name to make a quick profit. Likewise, they may seek to extort a ransom from you to get it back. However, there are many reasons that domain name hijacking is more dangerous than many forms of ordinary theft. A well-established, reputable domain name will generate traffic and profits for its owner every moment.

As a result, every moment that a malicious actor holds onto your domain name is a moment that your brand suffers lasting damage. It's even possible for the person who stole your domain name to use it to enrich themselves without selling it, or for them to covertly steal information without your awareness. Many of the unique risks of domain name hijacking lay in the potential for thieves to redirect traffic from your website.

Phishing

Phishing is one of the most well-known methods of social engineering that hackers will use to steal information. It generally consists of making something, such as an email or a login page look legitimate when the page is actually fake. Then, the goal

is to get people to input sensitive information on these fake pages, which will enable the malicious actor to steal and misuse it. **In the context of domain name hijacking theft, phishing is even more dangerous than normal. Domain name phishing can cost your customers untold amounts of money and destroy the reputation of your business.**

Domain name phishing consists of making a website that resembles the one they've stolen the domain name of. Then, when customers go to routinely access the website, they'll head to a convincing fake that's just waiting for them to input their data. It may result in the thieves stealing credit card information, passwords, and other valuable data from hundreds or thousands of people.

The reason that domain name phishing is especially dangerous is that the targets have virtually no way to avoid falling for it. When someone receives a phishing email, looking for details such as a correct domain name is key in identifying the scam and protecting yourself. When the domain name is correct and leads to a scam website, people will go about their normal online routines and become the principal victims of the scam. What's even worse is that the thief will be able to use their position as the owner of the domain to encourage those who use the website to go online and update or change the information on their accounts.

Communications Theft

Once a hacker has taken over your domain, they'll gain a vast level of control over your communication systems. Chat, email, and other forms of online communication will become subject to their whims. An actor who intends to cause chaos and damage your business might delete emails, disable certain forms of communication, or otherwise interfere with communication.

They'll also be able to use your network for their own purposes, such as advertising a different business or product. Domain name hijacking might result in a case of your network being exploited to send outbound spam, which may result in your company going on a blacklist and suffering reputation damage. However, it's also possible that the interloper will simply sit back and read your communications. If a website traffics in any sort of valuable information, then this is a huge opportunity for theft.

Domain Name Takeover

Domain name hijacking isn't always a complex, in-depth event with a broader scheme behind it. However, it doesn't have to be such a type of attack for domain name hijacking to have a disastrous result on your business. A hacker can exploit your domain name for their own profit in a manner as simple as accessing the domain control panels and transferring the domain name to a different website.

> In this case, your website will totally cease to receive any traffic. For an eCommerce business, for instance, this means a total loss of profits.

On the other hand, the attacker will be able to use your website to increase traffic to their own. Your customers will attempt to head to your website via its domain name, only to end up at some other page. **This can result in your customers being tricked into failing for scams, or it can simply damage the reputation of your business.** The earlier mention of eCommerce businesses was for a reason; this kind of enterprise has become a favorite target of hackers in recent years.

VPN.COM

Sign up with our #1 choice

- ✓ Experts in Premium Domains
- ✓ Ultra-Secure Transactions
- ✓ Commissions Starting at 15%
- ✓ Paid $1m for VPN.com
- ✓ Only Pay When We Succeed for You
- ✓ Completely Confidential Transactions

Acquire Your Premium Domain

Reverse Domain Name Hijacking



Domain name hijacking is a serious threat to any webmaster but it is important to keep reverse domain name hijacking in mind as well. However that raises the question of what exactly this sort of attack is. First it is worth understanding that people also refer to reverse domain name hijacking as reverse cybersquatting, and to understand what cybersquatting is.

What Is Cybersquatting?

It's easy to define cybersquatting, as the United States government has formally defined it in law. In accordance with the Anticybersquatting Consumer Protection Act, cybersquatting is essentially using a domain name to profiteer from another brand. This can look like someone registering a domain name that's highly close to the one that you use while offering similar products and services. Once you understand cybersquatting, it's easy to make the step to understanding reverse cybersquatting. Then you can easily claim back your domain name hijacking from cybersquatter.

Reverse Cybersquatting

Reverse domain name hijacking, or reverse cybersquatting, is essentially the act of someone unfairly charging you with cybersquatting. In general, the victim first becomes aware when a party contacts you and tries to claim that you're guilty of cybersquatting. If they're unable to get you to cede ownership of your property, then they'll threaten to file a complaint to ICAAN and attempt to have the organization transfer your domain name to them. Reverse cybersquatting is particularly complicated because of the fact that a wrongful accusation isn't necessarily bad faith and extortion, and the person may sincerely believe you're infringing on their trademark. Bad faith is an essential component of the ICAAN definition of reverse cybersquatting;

"**Using the UDRP in bad faith to attempt to deprive a registered domain-name holder of a domain name**."

UDRP case decisions are not legal decrees, but they do invoke the power that ICAAN holds to transfer domain names. In general, the greatest danger of reverse cybersquatting is that complacency may result in the other person winning the case. Even if you win, you still might end up spending a great deal of time and money on the case. If you are interested in buying a new domain and starting a new business, check out How to Choose the best domain registrar in 2023.

Protect Your Domain Names



Domain name hijacking and reverse cybersquatting have similar means of defense. Maintaining robust, detailed documentation proving your right to ownership of the domain name will help you regain it via legal action or UDRP in either case. To avoid conventional domain name hijacking, you can remain watchful and make sure that your accounts are secure and you don't fall victim to social engineering or hacking attacks. **While fending off a reverse domain name hijacking case or while seeking to regain your domain name, it's key to maintain documentation.** There are many types of relevant documents you can use to build your case and prove that you're the rightful owner.

Copies of registration records that show the history of you or your organization as the rightful registrant is the starting point. Every time you have a new registration record, you should make a copy of it. Billing records, email receipts, and other records that prove consistent ownership are also invaluable.

System logs, archives, and other records of the content you've published to your web domain are highly important if you want to prove that you're the rightful owner of the domain name. Anything that proves a history of use, lease of rights to the domain, and your history and rights as the registrant can bolster your case. To protect your domain name from domain name **hijacking** and cybersquatting.

My Domain Name Was Stolen. What Next?

Even if you have done everything right your domain name might still be stolen. In this event it is ideal that you have prepared your documentation and know what to do. If you have not the steps you should take remain largely the same.

Contact Your Registrar

First things first contact your registrar and establish that the domain name has been stolen. The exact powers they have to help you vary based on the company but it is important to make it known you believe your domain name has been stolen. This will help establish your case as you move forward with legal action or file with UDRP.

Find A Good Domain Name Attorney

To pursue litigation and have your domain name returned to you, you'll need a skilled attorney with relevant experience. Look into IP attorneys, trademark attorneys, and domain name attorneys in your area. **Be sure to shop around and look for qualifications and fair pricing, but emphasize the urgency of your situation.** An experienced attorney will be able to give you advice on the best way to proceed in your unique circumstances. Then domain name hijacking can be dealt with in legal ways. Domain Attorney can help you regain your domain from domain name hijacking.

Seek A Court Order

While ICAAN will often handle the process of returning your domain name to you, a court order can help hasten the process. Likewise, a strong case as prepared by

your attorney will improve the odds of having your domain name returned. Once you've fulfilled these steps, your odds of successfully regaining your domain name hinge on the overall strength of your case.

VPN.COM

Sign up with our #1 choice

- ✓ Experts in Premium Domains
- ✓ Ultra-Secure Transactions
- ✓ Commissions Starting at 15%
- ✓ Paid $1m for VPN.com
- ✓ Only Pay When We Succeed for You
- ✓ Completely Confidential Transactions

Acquire Your Premium Domain

Get Help Recovering Your Stolen Domain Name

Your domain name is a priceless possession that encompasses much of your hard work in establishing your brand reputation. Protecting users privacy and intellectual property rights are two of VPN.com top priorities. VPN.com and our premium domain services are ideal for anyone seeking information about domain name hijacking or assistance in selecting the ideal domain name.

Africa Domains

Country	Domain Extension	Language	Capital
Algeria	.dz	Arabic	Algiers
Angola	.co.ao	Portuguese	Luanda
Antarctica	.aq	Russian, English	N/A
Benin	.bj	French	Porto-Novo

Asia Domains

Country	Domain	Language	Capital
Afghanistan	.af	Pashto, Dari	Kabul
Armenia	.am	Armenian	Yerevan
Azerbaijan	.az	Azerbaijani	Baku
Bangladesh	.com.bd	Bengali	Dhaka
Bhutan	.bt	Dzongkha	Thimphu
British Indian	.io	English	Camp

Caribbean Domains

Country	Domain Extension	Language	Capital
Anguilla	.ai	English	The Valley
Antigua	.ag	English	Saint John's
Aruba	.aw	Dutch, Papiamento	Oranjestad
Bahamas	.bs	English	Nassau

Central America Domains

Country	Domain	Language	Capital
Belize	.bz	English	Belmopan
Costa Rica	.cr	Spanish	San José
El Salvador	.com.sv, .sv	Spanish	San Salvador
Guatemala	.com.gt, .gt	Spanish	Guatemala City

Europe Domains

Country	Domain Extension	Language	Capital
Aland Islands	.ax	Swedish	Mariehamn
Albania	.al	Albanian	Tirana
Ascension Island	.ac	English	Georgetown
Austria	.at	German	Vienna

Middle East Domains

Country	Domain	Language	Capital
Arab Emirates	.ae	Arabic	Abu Dhabi
Bahrain	.bh	Arabic	Manama
Iraq	.iq	Kurdish, Arabic	Baghdad
Israel	.co.il	Hebrew	Jerusalem

Oceania Domains

Country	Domain Extension	Language	Capital
American Samoa	.as	Samoan, English	Pago Pago
Australia	.com.au	English	Canberra
Cocos Islands	.cc	English	West Island
Australia	.com.au	English	Canberra
Cocos Islands	.cc	English	West Island
Cook Islands	.co.ck	Rarotongan,	Avarua

South America Domains

Country	Domain Extension	Language	Capital
Argentina	.ar, .com.ar	Spanish	Buenos Aires
Bolivia	.bo	Spanish	La Paz, Sucre
Bolivia	.bo	Spanish	La Paz, Sucre
Brazil	.com.br	Portuguese	Brasília
Chile	.cl	Spanish	Santiago